10/562664

R E P U B L I Q U E F R A N C A I S E

INPI

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

AP5 Rec'd PCT/PTO 28 DEC 2005

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 04 NOV. 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

CERTIFIED COPY OF PRIORITY DOCUMENT

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W/ 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE 1 JUIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0307947
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI - 1 JUIL. 2003

Vos références pour ce dossier *(facultatif)*

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET HERRBURGER
115, boulevard Haussmann

75008 PARIS

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Boîtier sécurisé renfermant un clavier permettant d'introduire des données confidentielles

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases)		☒ Personne morale ☐ Personne physique
Nom ou dénomination sociale		TOKHEIM SERVICES FRANCE
Prénoms		
Forme juridique		
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	9, avenue Galilée
	Code postal et ville	9 2 3 5 0 LE PLESSIS ROBINSON
	Pays	France
Nationalité		française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 1 JUIL 2003
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0307947

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		
Prénom		
Cabinet ou Société		CABINET HERRBURGER
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	115, boulevard Haussmann
	Code postal et ville	7 5 0 0 8 PARIS
	Pays	France
N° de téléphone *(facultatif)*		01 44 51 68 00
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
CABINET HERRBURGER
Pierre HERRBURGER
CPI 92-1114

VISA DE LA PRÉFECTURE OU DE L'INPI
L. MARIELLO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Domaine de l'invention

La présente invention concerne un boîtier sécurisé renfermant un clavier permettant d'introduire des données confidentielles telles qu'un numéro d'identification personnel, destinées en particulier à un système de paiement électronique.

Les circuits électroniques ont largement contribué au développement des sociétés modernes et sont utilisés dans de nombreux domaines de la technique.

Ces circuits ont en particulier permis la création et l'essor des systèmes dits « de paiement électronique » qui permettent d'effectuer diverses transactions à partir de terminaux de paiement électronique équipés de claviers numériques en utilisant des cartes de crédit.

Or, ces systèmes doivent être sécurisés de façon à protéger tant les clients que les commerçants en évitant tout risque de transactions frauduleuses.

Dans ce but, les banques et les fabricants de cartes de crédit attribuent à celles-ci des numéros d'identification personnels que leurs propriétaires doivent entrer dans le clavier numérique équipant les terminaux de paiement électronique.

Après leur introduction, les numéros d'identification ainsi que d'autres données confidentielles figurant sur les cartes de crédit sont cryptés dans des modules de sécurité préalablement à la transaction.

Le numéro d'identification personnel permet donc de vérifier que la carte de crédit est bien utilisée par son véritable propriétaire, et non par un intrus ayant trouvé ou volé celle-ci.

Pour des raisons évidentes de sécurité, il est essentiel qu'entre son introduction dans le clavier numérique d'un terminal de paiement électronique et son cryptage un numéro d'identification personnel ne soit pas accessible à des tiers malintentionnés.

Il est par suite nécessaire d'associer des dispositifs de protection à ces claviers.

Les fraudeurs font cependant preuve de plus en plus d'astuce pour tenter d'obtenir des données confidentielles et par suite la sécurisation des claviers numériques des terminaux de paiement électronique est de plus en plus difficile.

A titre d'exemple, les fraudeurs peuvent :

- visualiser la saisie d'un code confidentiel (directement ou par l'intermédiaire de systèmes vidéo) ;

- accéder à l'électronique du système, notamment en insérant dans celui-ci une carte électronique « moucharde » ;
- « écouter » les émissions électromagnétiques émises par l'électronique du système pour les corréler avec les touches appuyées ;
- voler les informations lorsqu'elles sont frappées, par exemple en posant un faux clavier au-dessus du clavier véritable, ou en répandant sur celui-ci une substance telle que de la poussière qui laisse des traces sur les touches utilisées.

Etat de la technique

Différents moyens ont déjà été proposés pour tenter de sécuriser les claviers numériques des terminaux de paiement électronique.

On a à titre d'exemple déjà proposé de dissimuler les touches des claviers des regards indiscrets (document WO 00/68859) ou encore de changer la position des touches à chaque nouvelle utilisation (document WO 98/27518).

Ces différents moyens rendent plus difficile la détermination des données confidentielles en regardant un utilisateur les taper sur un clavier numérique.

Il a également déjà été proposé d'enfermer le clavier, son contrôleur ainsi que le module de sécurité associé à celui-ci dans un boîtier scellé, de façon à interdire aux fraudeurs d'avoir accès au système électronique en amont du cryptage des données confidentielles introduites dans le clavier.

A titre d'exemple, on a déjà proposé conformément au document WO 01/92349 d'enfermer l'électronique entre le clavier et une plaque de verre.

De telles solutions s'avèrent cependant très onéreuses et particulièrement difficiles à mettre en œuvre.

Par suite, jusqu'à ce jour, il n'a pas été proposé de moyen de sécurisation sûr et satisfaisant sur le plan économique des claviers numériques des terminaux de systèmes de paiement électronique.

But de l'invention

La présente invention a pour objet de combler cette lacune en proposant un boîtier sécurisé renfermant un clavier numérique conçu de manière à empêcher les intrus de pouvoir accéder frauduleusement aux données confidentielles introduites avant leur cryptage par un module de sécurité.

L'invention a en particulier pour objet de permettre de détecter un dispositif placé sur le clavier afin de déterminer les données confidentielles entrées, ou de prévenir toute altération du système effectuée dans le même but.

Un autre objet de l'invention est d'empêcher toute écoute des émissions électromagnétiques générées par l'électronique du système.

Le boîtier qui fait l'objet de l'invention est tout spécialement adapté à la sécurisation des claviers numériques équipant les terminaux de paiement des systèmes de paiement électronique mais peut s'adapter à la sécurisation de tout système dans lequel des données confidentielles sont transmises par clavier.

Exposé de l'invention

Le boîtier sécurisé qui fait l'objet de l'invention est caractérisé en ce qu'il comporte une matrice tactile capacitive reliée d'une part par des fils de liaison à une carte de circuit imprimé portant le contrôleur associé, un module de sécurité ainsi qu'une électronique sensible aux variations de la capacité du système, et prise d'autre part en sandwich entre deux plaques de verre, à savoir une plaque de verre avant ou plaque de protection et une plaque de verre arrière ou plaque de support.

Selon l'invention on utilise donc les propriétés des écrans tactiles capacitifs, bien connus de l'homme du métier, pour détecter la présence d'un dispositif extérieur fixé sur le clavier numérique, comme par exemple un faux clavier ou une substance déposée afin de marquer les touches enfoncées lors de la saisie du code confidentiel.

Le clavier numérique est affiché au dessous des plaques de verre par un dispositif quelconque tel qu'écran LCD, CRT, LED, autocollant, ... et est lu par transparence.

Pour introduire son code confidentiel l'utilisateur touche avec ses doigts la plaque de protection au dessous de laquelle le clavier est affiché.

Cette manipulation a pour conséquence de changer localement la capacité du système, ce qui permet au contrôleur de connaître la position touchée donc de déterminer le code confidentiel introduit.

Il s'agit là du fonctionnement classique d'un écran tactile capacitif.

Pour que le système de sécurisation conforme à l'invention puisse fonctionner de manière satisfaisante, il est bien entendu nécessaire d'avoir déterminé lors d'une étape d'étalonnage préalable mise en œuvre

pendant la fabrication du boîtier, la capacité du système au repos (au repos signifiant qu'il n'y a aucun objet à côté ou sur l'écran tactile) au niveau des différents emplacements de la plaque de protection, correspondant aux différentes touches du clavier.

La liste de ces valeurs de capacité est enregistrée dans une mémoire en tant que référence.

Toute tentative de « masquage » du clavier dans un but frauduleux modifie la capacité du système.

Par suite, en cours de fonctionnement les valeurs réelles de capacité sont constamment comparées aux valeurs enregistrées et toute déviation supérieure à un niveau de déviation autorisé prédéterminé est interprétée comme indicative d'une fraude et déclenche une alarme ou l'arrêt du système.

Selon une autre caractéristique de l'invention, la carte de circuit imprimé est située à proximité immédiate de la matrice tactile capacitive et est recouverte par la plaque de protection.

Cette caractéristique permet aux fils de liaison de la matrice tactile capacitive et de la carte de circuit imprimé d'être aussi courts que possible, ce qui a pour résultat d'interdire l'accès aux circuits où transitent des données confidentielles non sécurisées.

Selon une autre caractéristique de l'invention, la carte de circuit imprimé et les composants électroniques fixés sur celle-ci sont noyés dans une résine cassante, notamment une résine époxy.

Cette caractéristique permet de garantir que les fils reliant les différents composants électroniques soient automatiquement brisés en cas d'attaque physique, notamment de tentative de « poinçonnage » des plaques de verre.

Selon une autre caractéristique de l'invention, la plaque de support est recouverte, sur sa face arrière, d'une troisième plaque de verre ou plaque de recouvrement se prolongeant au niveau de la face arrière de la carte de circuit imprimé.

La présence de cette plaque de recouvrement permet d'améliorer la sécurisation de la carte de circuit imprimé.

Selon l'invention, la plaque de protection, la plaque support et le cas échéant, la plaque de recouvrement sont de préférence réalisées en un verre cassant.

Cette caractéristique contribue à interdire à un intrus d'avoir accès à des données confidentielles non sécurisées en aval de la plaque de protection.

En effet, toute tentative dans ce sens aurait pour conséquence de casser les différentes plaques de verre et/ ou la résine cassante dans laquelle est noyée la carte de circuit imprimé, et par suite d'endommager l'électronique du système et de détruire les données confidentielles qu'elle contient.

Selon une caractéristique préférentielle de l'invention, le boîtier sécurisé renferme un circuit de détection de fraudes comportant une source de tension, un conducteur électrique accolé à une plaquesde verre, ainsi qu'un détecteur de courant associé à un organe d'alarme.

Le conducteur électrique peut être constitué par un long fil ou une métallisation d'une plaque de verre en forme de boucle.

Toute tentative d'accès aux parties sensibles du boîtier sécurisé (module de sécurité par exemple) entraîne la fragmentation des plaques de verre et par suite la rupture du conducteur qui est immédiatement détectée par le détecteur de courant et interrompt l'alimentation d'une mémoire de sauvegarde de paramètres de fonctionnement du clavier stockés lors de la fabrication.

La détection de cette rupture entraîne une alarme et avantageusement la désactivation du système.

Selon une autre caractéristique particulièrement avantageuse de l'invention, le circuit de détection de fraudes est parcouru par un courant oscillant à haute fréquence modulé en amplitude et en fréquence de façon à provoquer un brouillage des émissions électromagnétiques du système vis-à-vis de l'extérieur et à empêcher ainsi toute tentative de lecture des signaux internes du système à l'aide d'un récepteur haute fréquence extérieur.

Selon l'invention, on peut également prévoir d'autres organes de sécurisation du boîtier, par exemple associer à l'écran un filtre optique standard connu en lui-même de façon à permettre de réduire l'angle de vision sur lequel le clavier peut être lu.

Dessins

Les caractéristiques du boîtier sécurisé qui fait l'objet de l'invention seront décrites plus en détail en se référant aux dessins annexés dans lesquels :

- la figure 1 est une perspective « éclatée » schématique illustrant la configuration du boîtier sécurisé ;
- la figure 1a est un schéma illustratif du mode d'utilisation du boîtier ;
- la figure 1b est un schéma illustratif d'une tentative de fraude ;
- la figure 2 est un schéma représentant le circuit de détection de fraudes.

Description de modes de réalisation

Selon la figure 1, le boîtier sécurisé 1 comporte une matrice tactile capacitive prise en sandwich entre deux plaques réalisées en un verre cassant à savoir une plaque de protection 3 et une plaque de support 5.

La matrice tactile capacitive 2 est reliée par des fils de liaison 6 à une carte de circuit imprimé 7 portant le contrôleur associé, un module de sécurité 16 (figure 2) ainsi qu'une électronique sensible aux variations de la capacité du système.

La carte de circuit imprimé 7 et les composants électroniques fixés sur celle-ci sont noyés dans une résine époxy cassante 8.

Comme représenté sur la figure 1, la carte de circuit imprimé 7 est située à proximité immédiate de la matrice tactile capacitive 2 et est recouverte par la plaque de protection 3 dont la longueur est supérieure à celle de la plaque de support 5.

La plaque de support 5 peut le cas échéant être recouverte sur sa face arrière opposée à la plaque de protection 3 par une troisième plaque de verre non représentée sur les figures, à savoir une plaque de recouvrement se prolongeant au niveau de la face arrière de la carte de circuit imprimé 7.

Cette configuration permet de réduire au maximum le trajet dans lequel transitent des données confidentielles non sécurisées après leur introduction dans le boîtier 1.

En effet, à la sortie du boîtier 1, ces données ont subi un cryptage leur évitant d'être interceptées par un fraudeur.

Il est à noter que conformément à l'exemple de réalisation représenté sur les figures, la matrice tactile fonctionne selon la technologie classique des écrans tactiles capacitifs projetés.

Par suite la matrice tactile est constituée par une matrice de fins micro fils connectés au contrôleur.

Une fréquence d'oscillation est assignée à chacun de ces micro fils.

Selon la figure 1a, pendant une utilisation normale, l'utilisateur touche avec ses doigts la plaque de protection 3 au travers de laquelle le clavier est affiché par un dispositif d'affichage 4.

Le fait de toucher la plaque de protection 3 modifie la fréquence d'oscillation des micro fils situés à l'emplacement correspondant.

Cette modification qui est une fonction de la capacité du système permet au contrôleur fixé sur la carte de circuit imprimé 7 de déterminer à quel endroit la plaque de protection 3 et par suite l'écran projeté a été touché par l'utilisateur, et donc de déterminer le code confidentiel introduit.

Lors d'une étape d'étalonnage préalable on a mesuré la capacité au repos au niveau de chaque croisement de fils de la matrice tactile 7.

La liste des valeurs ainsi mesurées est enregistrée en tant que référence dans une mémoire 9 associée au module de sécurité 16 d'une façon représentée schématiquement sur la figure 2.

Selon la figure 1b, si un intrus applique sur la plaque de protection 3 un dispositif de « marquage » 10 tel que faux clavier ou couche de poussière à des fins frauduleuses, la capacité réelle du système est modifiée et cette modification est constatée par l'électronique de commande qui peut en réponse générer une alarme ou arrêter le système.

Bien entendu, l'invention pourrait être transposée à de nombreuses autres technologies d'écrans tactiles capacitifs sans pour cela sortie du cadre de celle-ci.

Selon la figure 2, le boîtier 1 renferme en outre un circuit de détection de fraudes 11 comportant essentiellement une source de tension 12 ainsi qu'un conducteur électrique en forme de boucle 13 accolé à la plaque de protection 3.

Ce circuit 11 renferme également un détecteur de courant 14 associé à un organe d'alarme non représenté.

Une tentative d'accès aux parties sensibles du boîtier, notamment à la carte de circuit imprimé 7 a pour conséquence de casser la plaque de protection 3 et par suite de rompre le conducteur 13 entraînant ainsi l'émission d'une alarme, et également la désactivation du système par suite de l'effacement de la mémoire 9.

Selon la figure 2, le circuit de détection de fraudes 11 est également équipé d'un dispositif de protection 15 permettant d'alimenter ce circuit en un courant oscillant à haute fréquence modulé en amplitude

et en fréquence de façon à provoquer un brouillage des émissions électromagnétiques du système vis-à-vis de l'extérieur.

REVENDICATIONS

1°) Boîtier sécurisé renfermant un clavier permettant d'introduire des données confidentielles telles qu'un numéro d'identification personnel destinées en particulier à un système de paiement électronique,
caractérisé en ce qu'
il comporte une matrice tactile capacitive (2) reliée d'une part par des fils de liaison (6) à une carte de circuit imprimé (7) portant le contrôleur associé, un module de sécurité (16) ainsi qu'une électronique sensible aux variations de la capacité du système, et prise d'autre part en sandwich entre deux plaques de verre, à savoir une plaque de verre avant ou plaque de protection (3) et une plaque de verre arrière ou plaque de support (5).

2°) Boîtier sécurisé selon la revendication 1,
caractérisé en ce que
la carte de circuit imprimé (7) est située à proximité immédiate de la matrice tactile capacitive (2) et est recouverte par la plaque de protection (3).

3°) Boîtier sécurisé selon l'une quelconque des revendications 1 et 2,
caractérisé en ce que
la carte de circuit imprimé (7) et les composants électroniques fixés sur celle-ci sont noyés dans une résine cassante, notamment une résine époxy (8).

4°) Boîtier sécurisé selon l'une quelconque des revendications 1 à 3,
caractérisé en ce que
la plaque de support (5) est recouverte sur sa face arrière d'une troisième plaque de verre ou plaque de recouvrement se prolongeant au niveau de la face arrière de la carte de circuit imprimé (7).

5°) Boîtier sécurisé selon l'une quelconque des revendications 1 à 4,
caractérisé en ce que
la plaque de protection (3), la plaque de support (5) et le cas échéant la plaque de recouvrement sont réalisées en un verre cassant.

6°) Boîtier sécurisé selon l'une quelconque des revendications 1 à 5,
caractérisé en ce qu'

REVENDICATIONS

1°) Boîtier sécurisé permettant d'introduire des données confidentielles telles qu'un numéro d'identification personnel destiné en particulier à un système de paiement électronique et comportant une matrice tactile capacitive (2) reliée d'une part par des fils de liaison (6) à une carte de circuit imprimé (7) portant un contrôleur associé, un module de sécurité (16) ainsi qu'une électronique sensible aux variations de la capacité du système, et prise d'autre part en sandwich entre deux plaques de verre, à savoir une plaque de verre avant ou plaque de protection (3) et une plaque de verre arrière ou plaque de support (5),
caractérisé en ce que
la plaque de protection (3) est réalisée en un verre fragmentable et est équipée d'un conducteur électrique (13) constitué par un long fil accolé à celle-ci ou par une métallisation en forme de boucle, ce conducteur électrique faisant d'une part partie d'un circuit de détection de fraudes (11) comportant une source de tension (12) ainsi qu'un détecteur de courant (14) associé à un organe d'alarme, et se rompant d'autre part sous l'effet d'une fragmentation de la plaque de protection (3) pour entraîner l'interruption du courant dans le circuit de détection de fraudes (11) et l'activation de l'organe d'alarme.

2°) Boîtier sécurisé selon la revendication 1,
caractérisé en ce que
la plaque de support (5) est elle aussi réalisée en un verre fragmentable et équipée d'un conducteur électrique faisant partie du circuit de détection de fraudes (11) et se rompant sous l'effet d'une fragmentation de celle-ci pour entraîner l'interruption du courant dans le circuit de détection de fraude (11) et l'activation de l'organe d'alarme.

3°) Boîtier sécurisé selon l'une quelconque des revendications 1 et 2,
caractérisé en ce que
la plaque de support (5) est recouverte sur sa face arrière d'une troisième plaque de verre ou plaque de recouvrement se prolongeant au niveau de la face arrière de la carte de circuit imprimé.

4°) Boîtier sécurisé selon la revendication 3,
caractérisé en ce que
la plaque de recouvrement est elle aussi réalisée en un verre fragmentable

il renferme un circuit de détection de fraudes (11) comportant une source de tension (12), un conducteur électrique (13) accolé à une plaque de verre (3) ainsi qu'un détecteur de courant (14) associé à un organe d'alarme.

7°) Boîtier sécurisé selon la revendication 6,
caractérisé en ce que
le circuit de détection de fraudes (11) est parcouru par un courant oscillant à haute fréquence modulé en amplitude et en fréquence de façon à provoquer un brouillage des émissions électromagnétiques du système vis-à-vis de l'extérieur.

et équipée d'un conducteur électrique faisant partie du circuit de détection de fraudes (11) et se rompant sous l'effet d'une fragmentation de celle-ci pour entraîner l'interruption du courant dans le circuit de détection de fraudes (11) et l'activation de l'organe d'alarme.

5°) Boîtier selon l'une quelconque des revendications 1 à 4,
caractérisé en ce que
la carte de circuit imprimé (7) est située à proximité immédiate de la matrice tactile capacitive (2) recouverte par la plaque de protection (3).

6°) Boîtier sécurisé selon l'une quelconque des revendications 1 à 5, la carte de circuit imprimé (7) et les composants électroniques fixés sur celle-ci sont noyés dans une résine cassante, notamment une résine époxy (8).

7°) Boîtier selon l'une quelconque des revendications 1 à 6,
caractérisé en ce que
le circuit de détection de fraudes (11) est parcouru par un courant oscillant à haute fréquence modulé en amplitude et en fréquence de façon à provoquer un brouillage des émissions électromagnétiques du système vis à vis de l'extérieur.

Figure 1

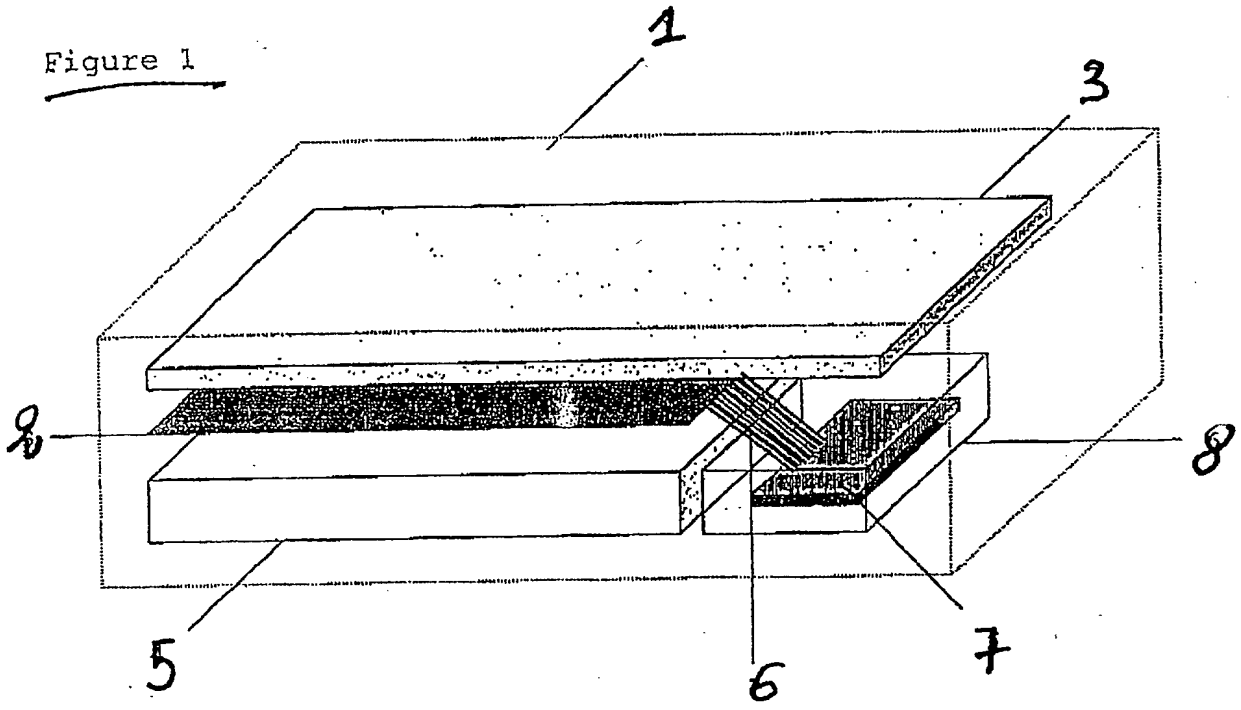
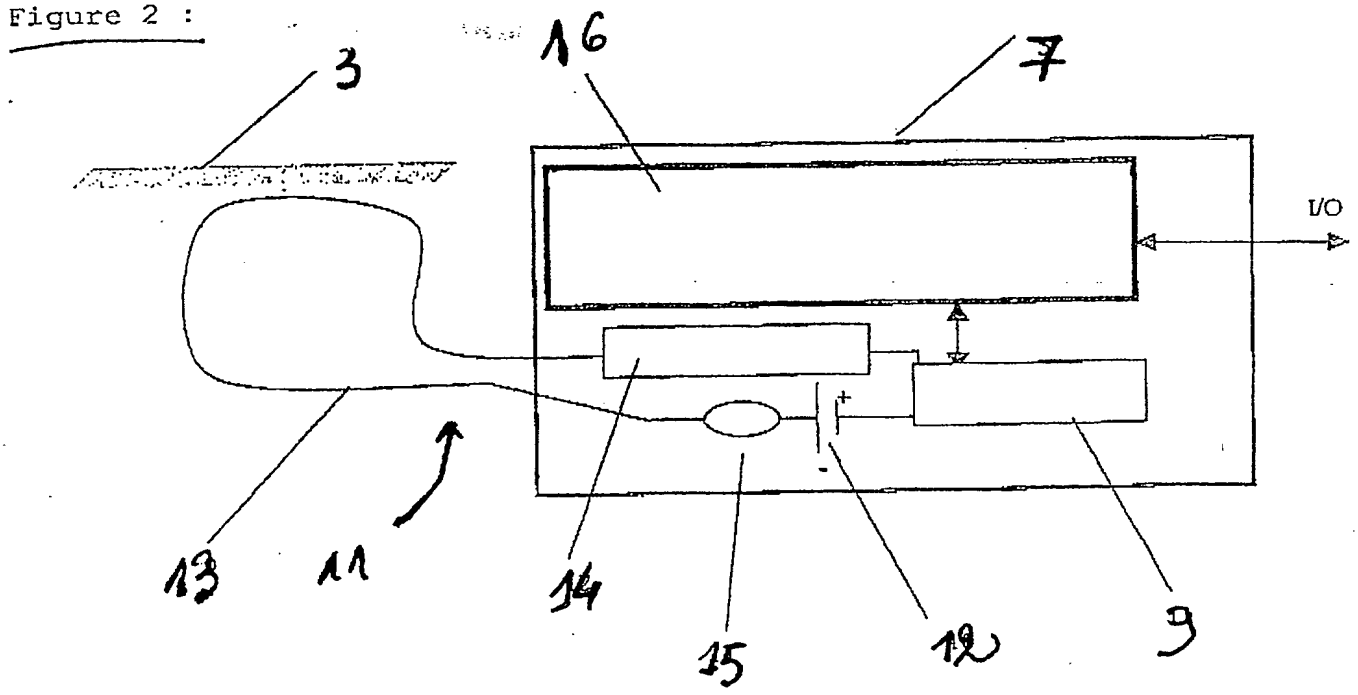


Figure 2 :



reçue le 01/09/03

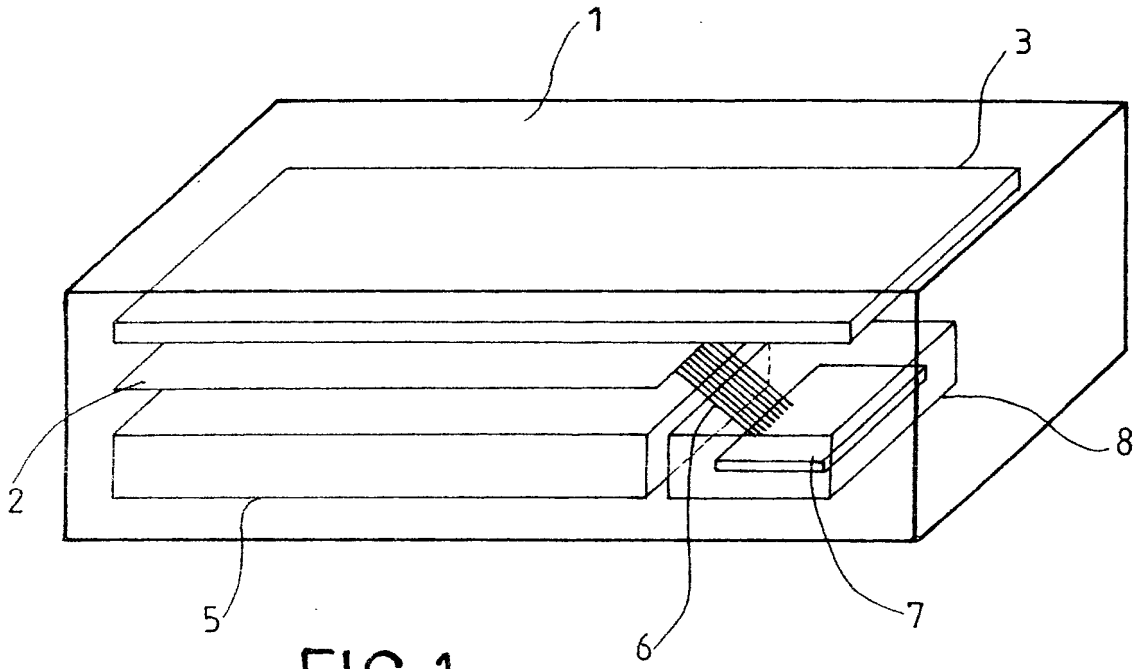


FIG.1

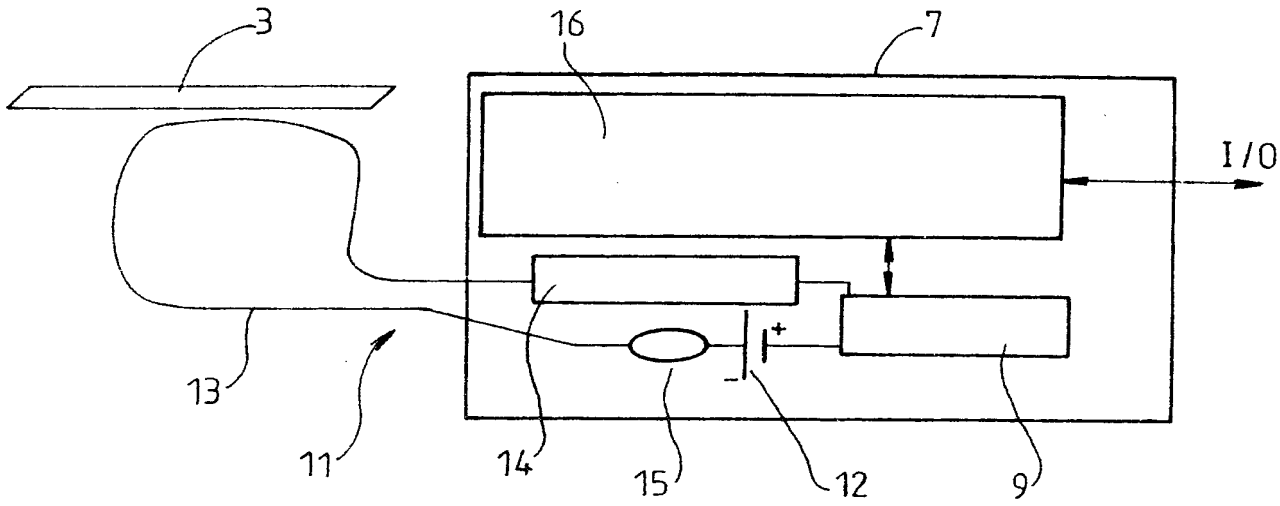


FIG.2

Figure 1a

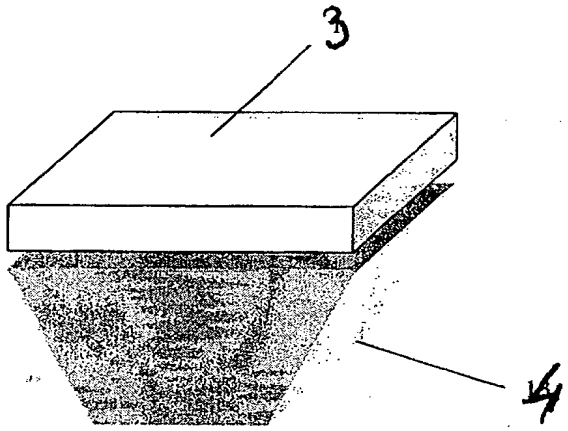
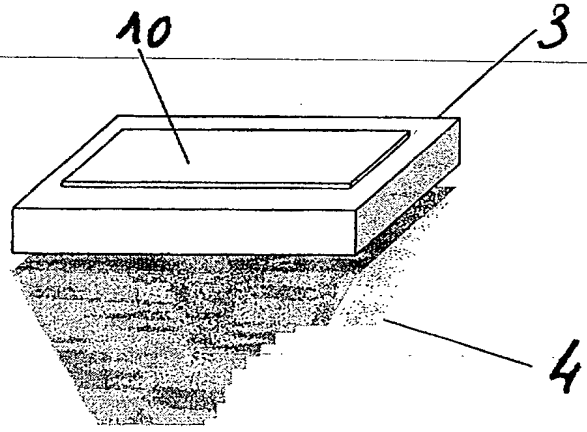


Figure 1b:



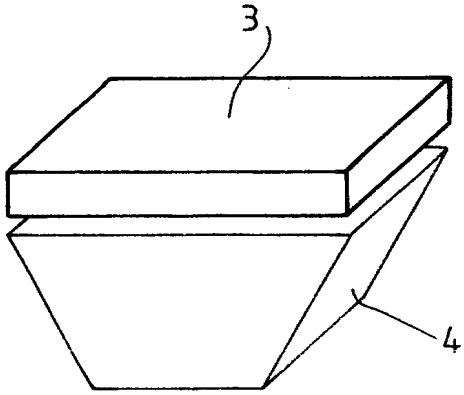


FIG.1a

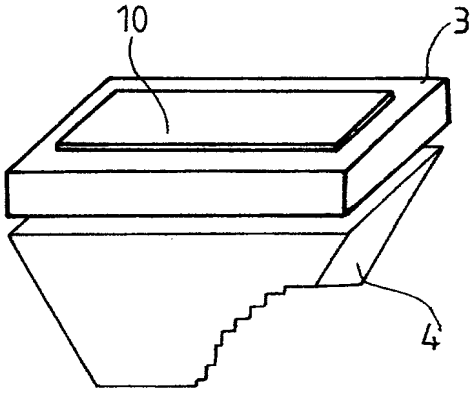


FIG.1b

reçue le 24/07/03

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	
N° D'ENREGISTREMENT NATIONAL	0307947

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Boîtier sécurisé renfermant un clavier permettant d'introduire des données confidentielles

LE(S) DEMANDEUR(S) :

TOKHEIM SERVICES FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		van de Kamer
Prénoms		Johan
Adresse	Rue	1, rue des pres
	Code postal et ville	1 4 1 2 0 Mondeville (France)
Société d'appartenance *(facultatif)*		
2 Nom		Heesters
Prénoms		Frans
Adresse	Rue	Zeegstraat 50
	Code postal et ville	5 5 4 1 EX REUSEL (Hollande)
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

01.07.2003
CABINET HERRBURGER
Pierre HERRBURGER
CPI 92-1114

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.